Qualys Security Conference Dubai

A 360° Approach to Securing the Cloud

Total Visibility and Comprehensive Security for Cloud workloads and infrastructure

Hari Srinivasan
Director Product Management, Qualys, Inc.

Agenda

Your responsibility in cloud security

Qualys Security for hardening and standardizing workloads

Qualys security for Infrastructure

Qualys security for SaaS

Use Cases & Demo

Q&A

Customer’s landscape is changing

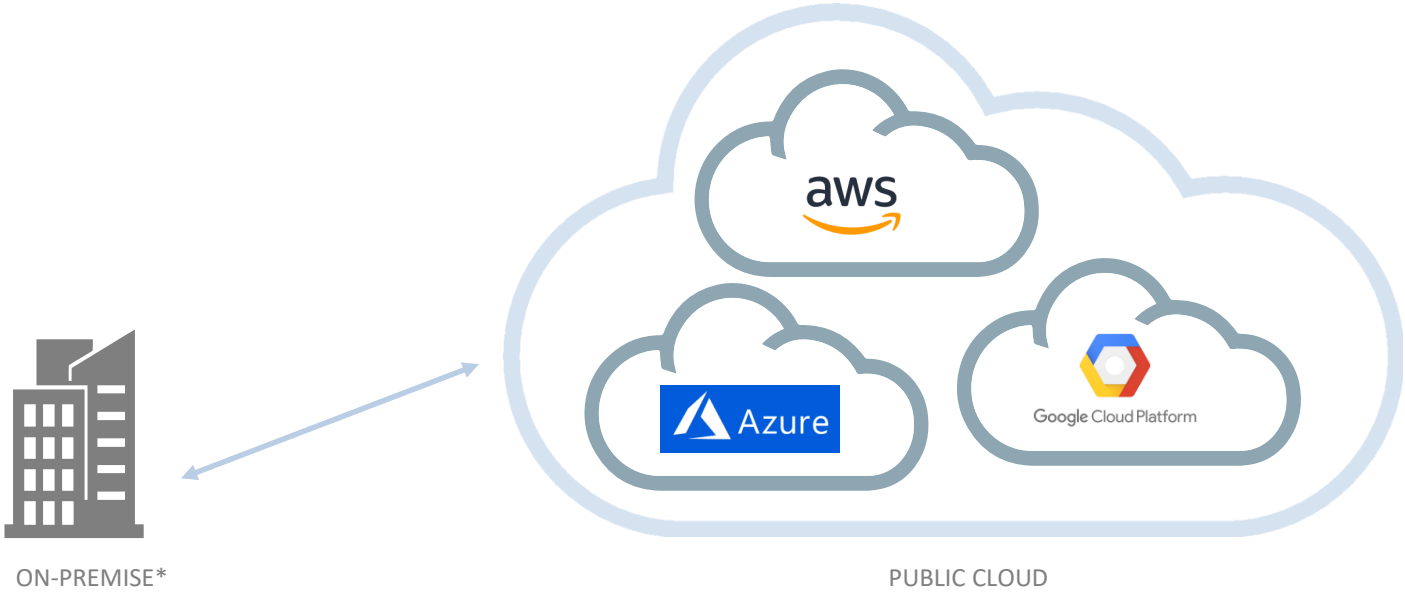
Bahrain Institute of Public Administration has moved their Learning Management System to AWS, reducing cost by 90%

Bahrain IGA is taking a cloud first policy migrating 700 servers with more than 50 TB data to AWS

معهد الإدارة العامة
Institute of Public Administration

Qualys.

The New IT – Hybrid, Multi-Cloud Deployment

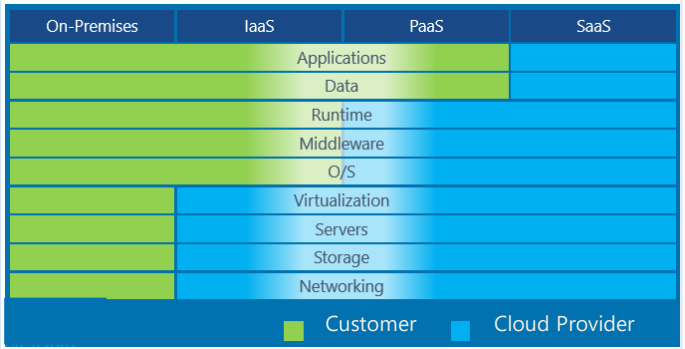


Qualys.

Shared Security Responsibility Model

You

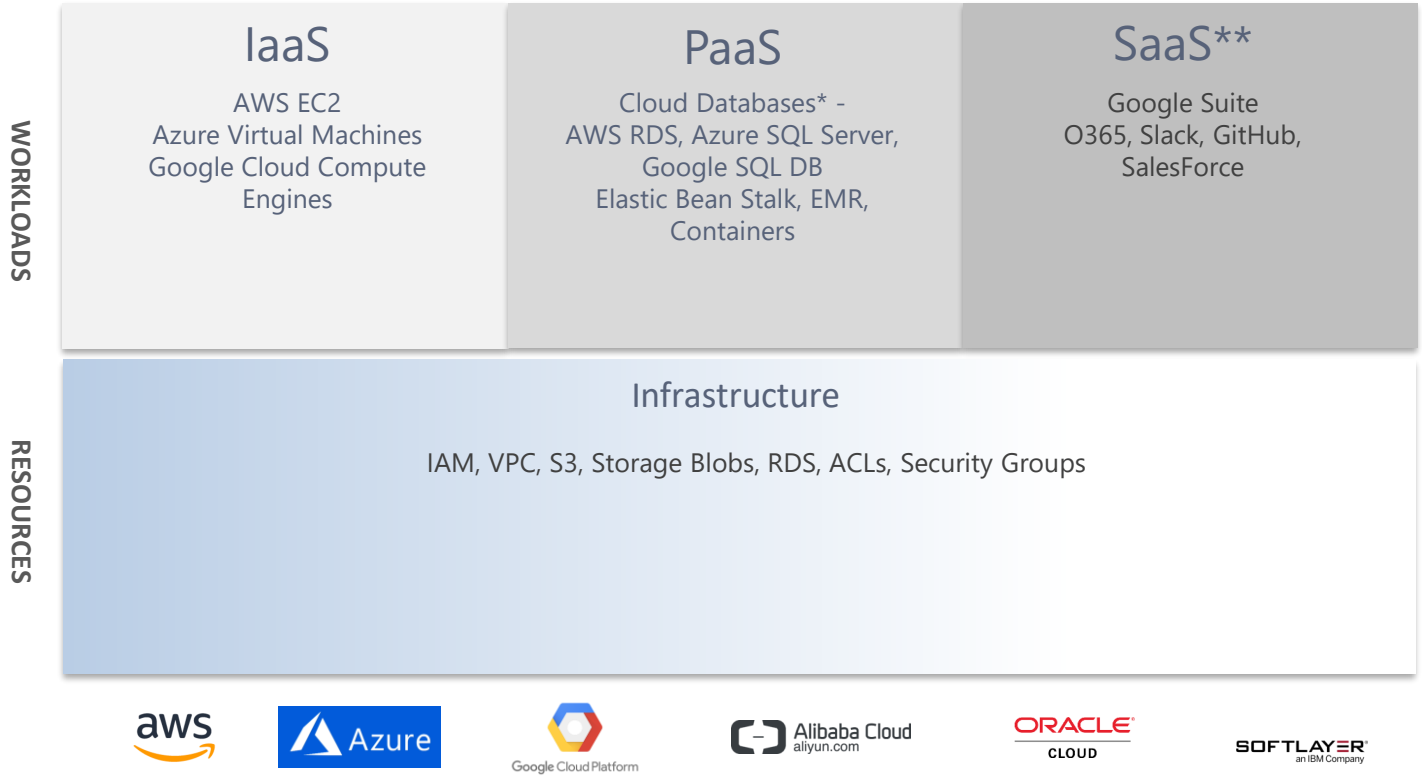
are responsible for securing your data and workloads



Varies by layers

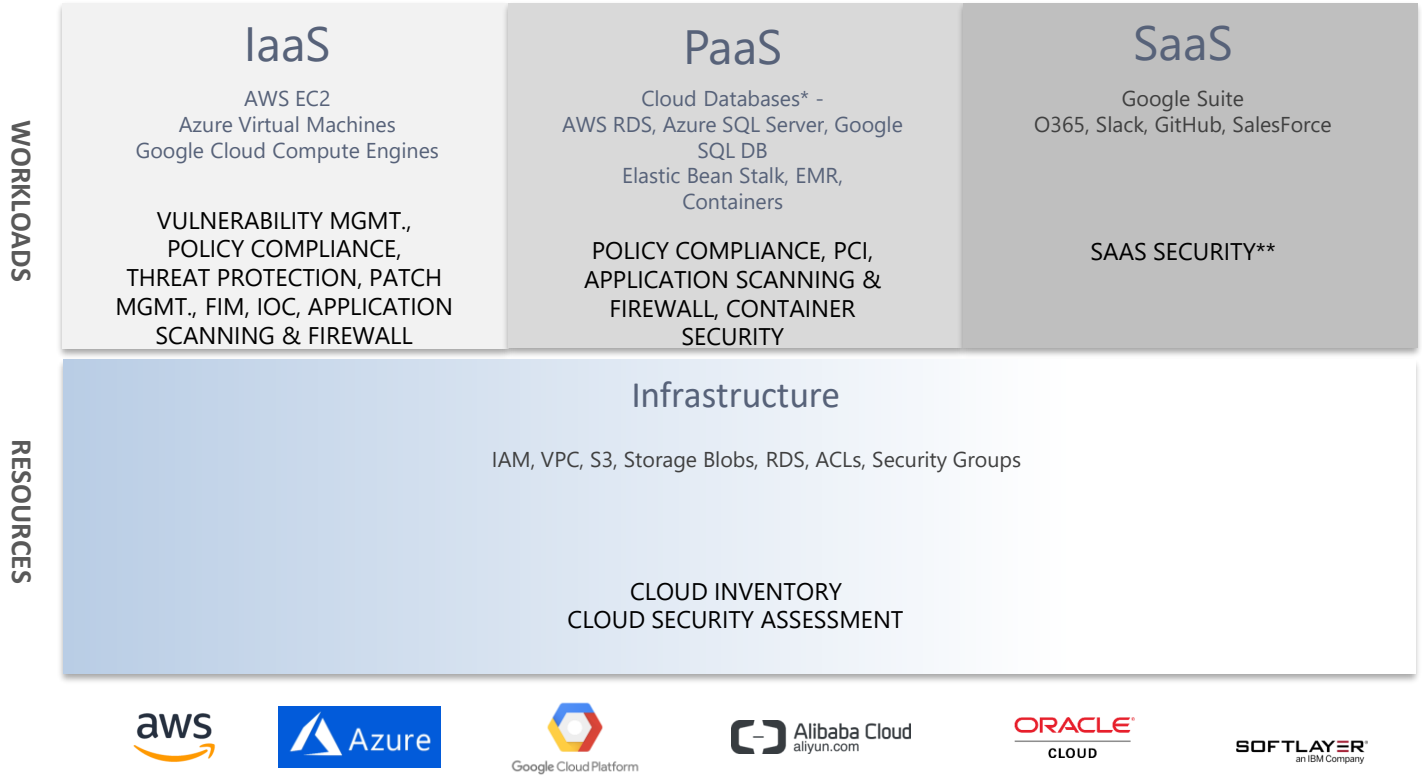
Image from Microsoft Azure Shared Security Responsibility

Components of Cloud Security



* PaaS – Cloud Database Scanning – Roadmap '19
** SaaS – Qualys acquired Adya.io Feb'19. Security for GSuite, Slack, O365,..

Components of Cloud Security



* PaaS – Cloud Database Scanning – Roadmap ‘19
** SaaS – Qualys acquired Adya.io Feb’19. Security for GSuite, Slack, O365,..

Qualys Sensors for Public Clouds

VIRTUAL SCANNER APPLIANCES

Remote scan across your networks – hosts and applications

CLOUD AGENTS

Continuous Security View and platform for additional security solutions

CLOUD CONNECTORS

Sync. cloud instances
And its metadata

INTERNET SCANNERS

Perimeter scan for edge facing Instances/Host and URLs

WEB APPLICATION FIREWALLS

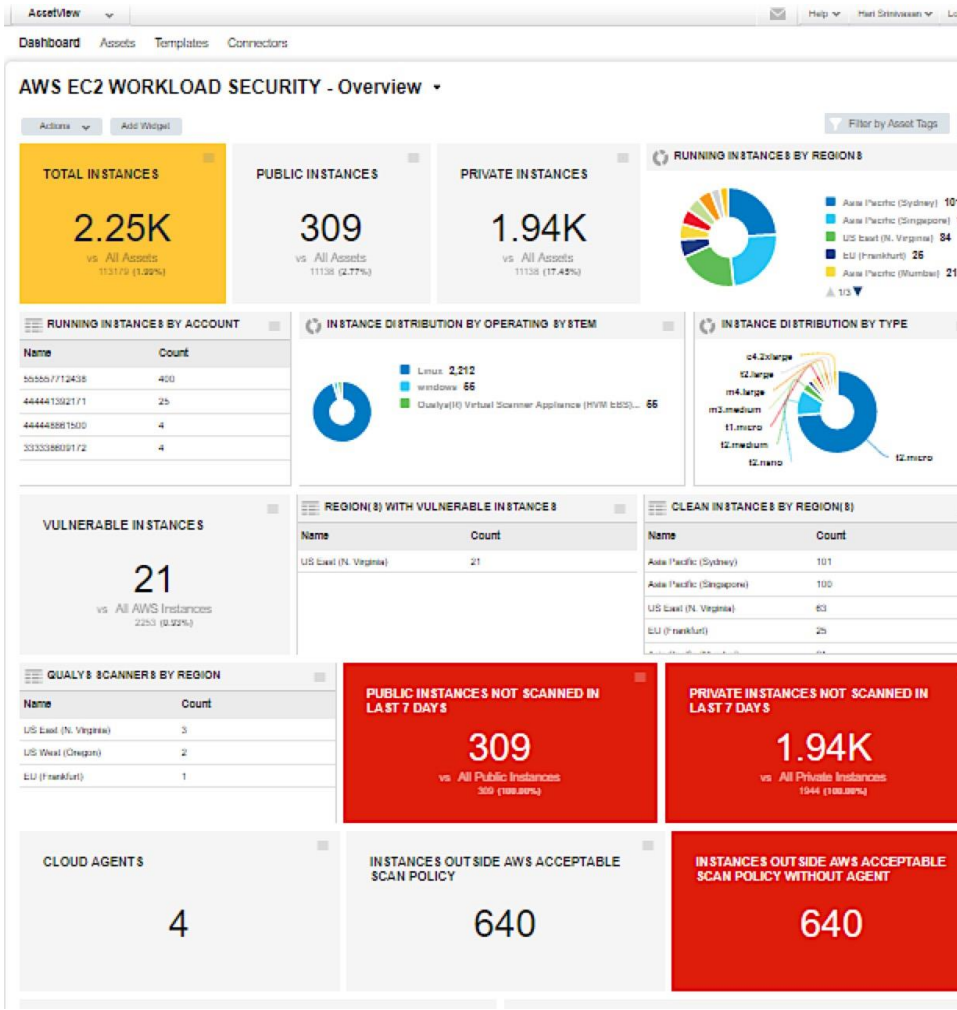
Actively defend intrusions and secure applications

Cloud Inventory & Security Posture Dashboard

Visibility into your cloud instances inventory

Identify your security coverage

View Security posture



Cloud Workload Security

Securing Cloud Workloads

Hardening and Standardizing

VULNERABILITY MANAGEMENT

- Vulnerability Management (Internal & Perimeter)
- Threat Protection
- Indicators of Compromise
- Patch Management*

POLICY COMPLIANCE

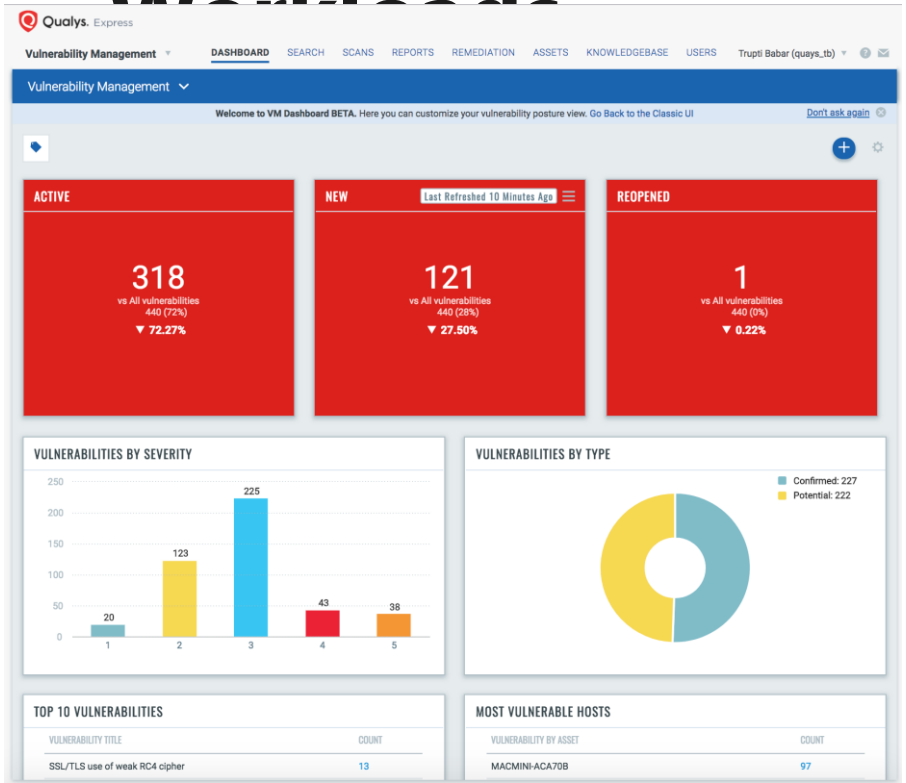
- Policy Compliance (incl. Secure Configuration Assessments)
- File Integrity Monitoring

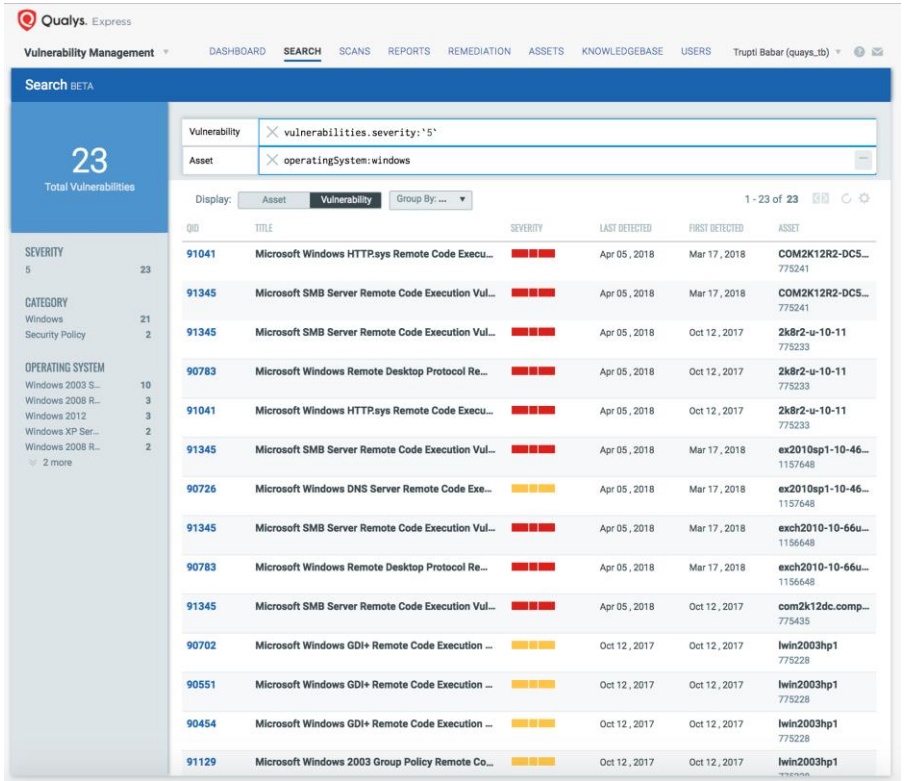
APPLICATION SECURITY

- Web Application Scanning (WebApps and REST APIs)
- Web Application Firewall

* Upcoming feature

Vulnerability Mgmt. for Cloud Workloads



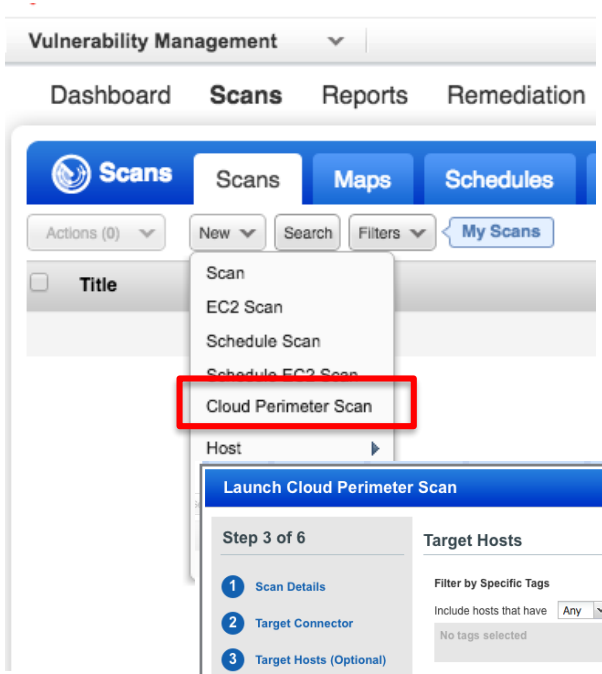


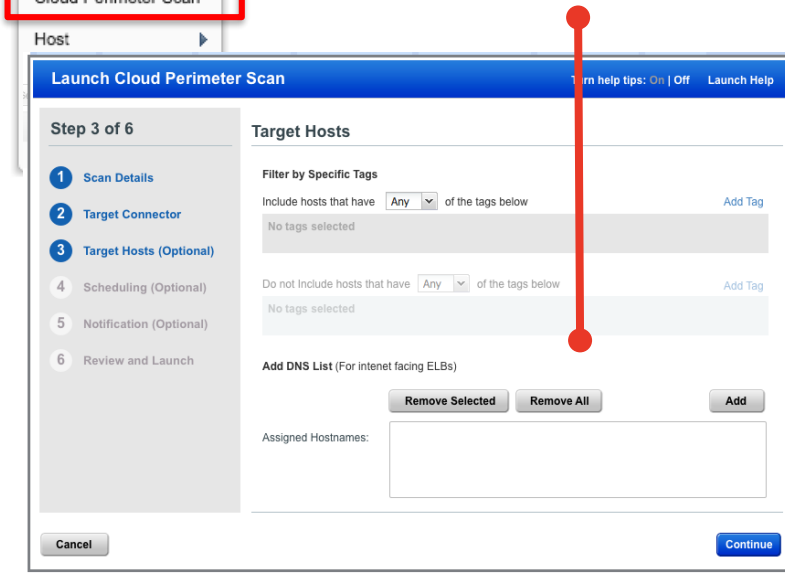
Qualys.

Vulnerability Mgmt. - External / Perimeter Workloads

Get a hacker's eye view of your public facing cloud environment

Runs remote check vulnerabilities like password brute force, port checks,..



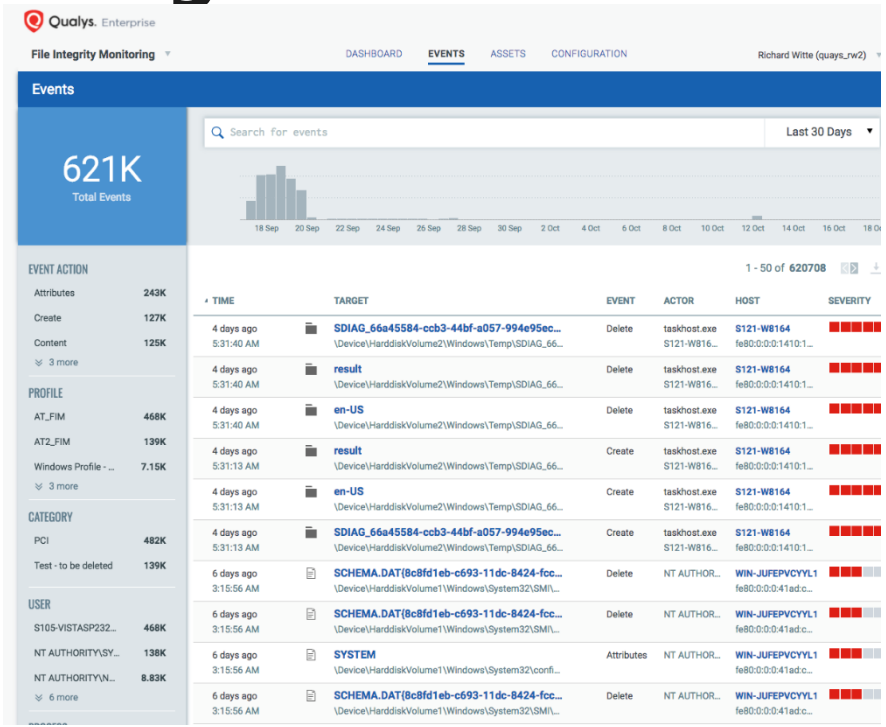


Auto selects Public Instances.

Add Load Balancer's DNS

Qualys.

Comprehensive Compliance Management & File Integrity Monitoring

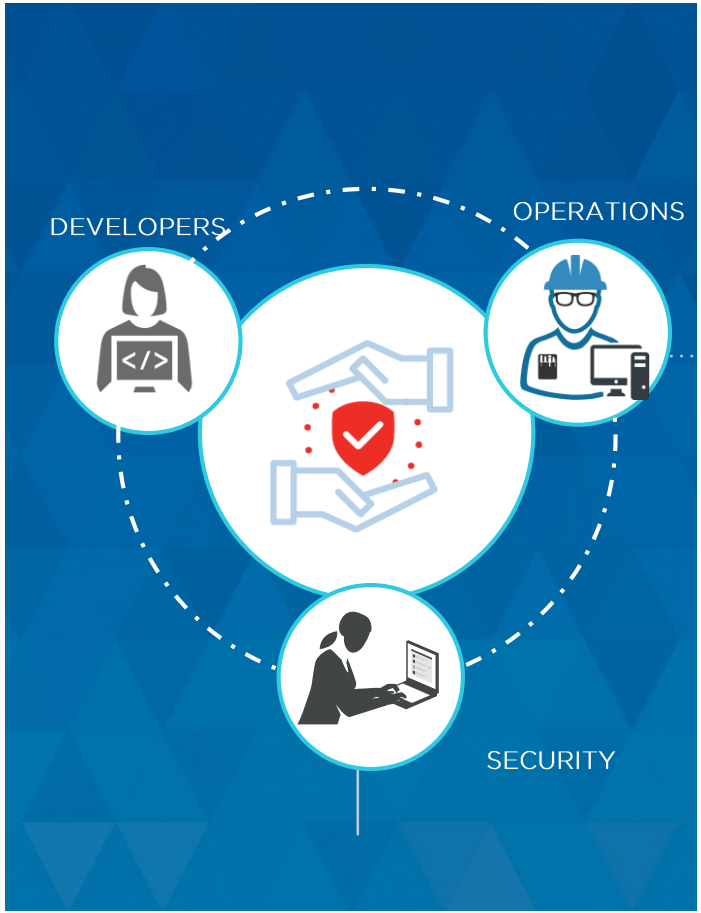


Moving Toward the Future of Security

Collaborative, Continuous Secure Development and Deployment

- ✓Static Code Analysis
- ✓Vulnerability Management
- ✓Compliance Checks
- ✓Web Application Scanning
- ✓Configuration Assessments

Comprehensive evaluation at an early stage **(DevOps)**



Qualys.

Securing Public Clouds Using Qualys

Customer Case Studies

Reduced application releases from 2 weeks to 24 hrs by automating security with Qualys in to DevOps

A SOFTWARE MAKER

Private

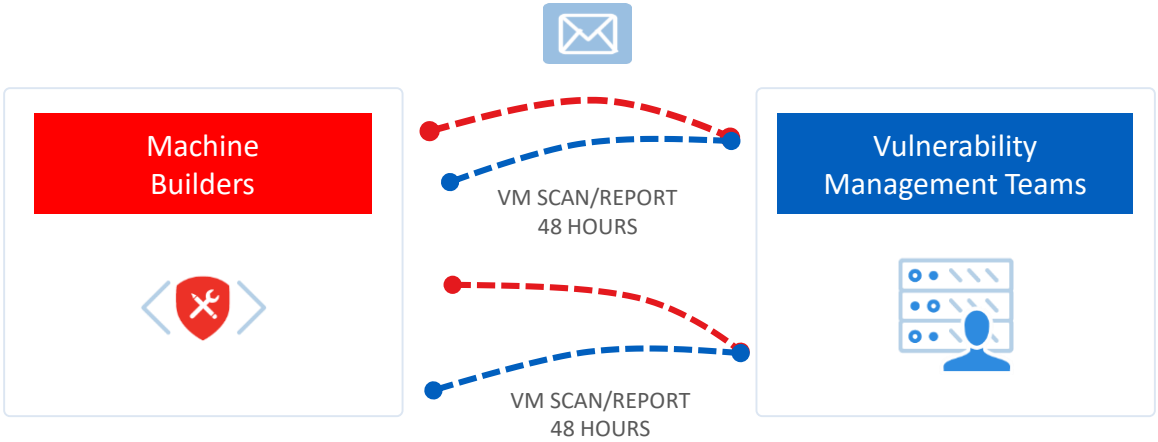
"Just in time" security approvals with end to End integration of Qualys Scan and Reports with Service Now,

A BEVERAGE MNC

Private

Enabling DevOps with automated agent deployment via Azure Security Center

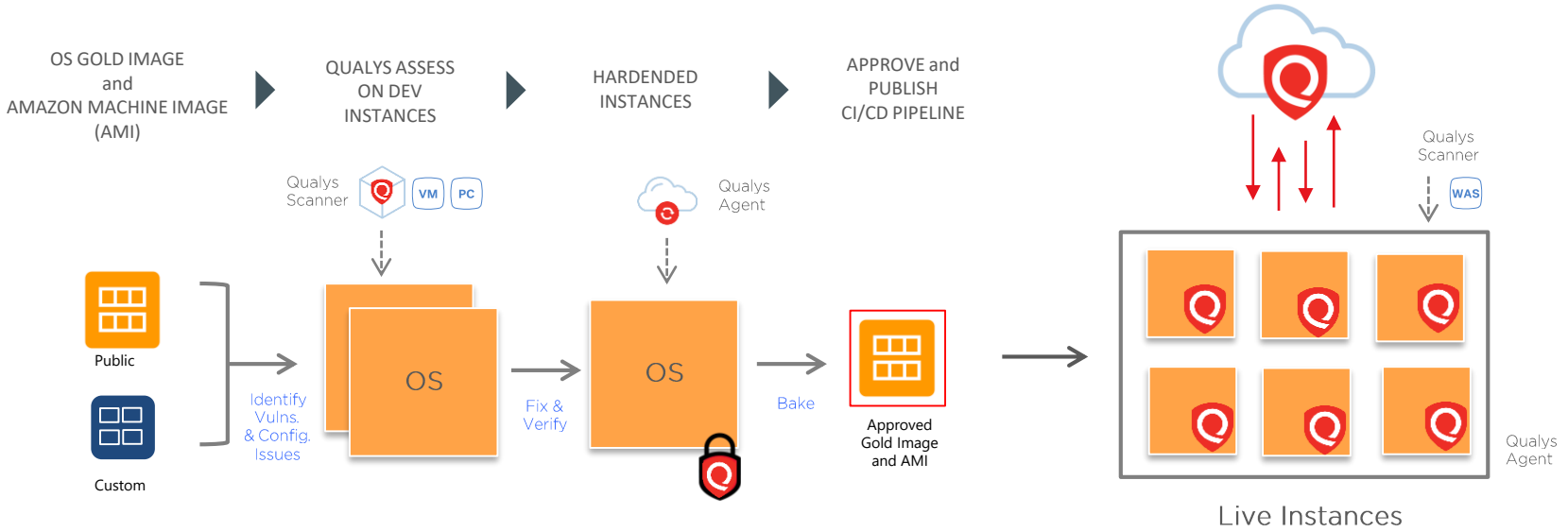
Capital One
Before: Lack of Security Automation Delays Release



Two weeks until the Image (AMI) is certified for production

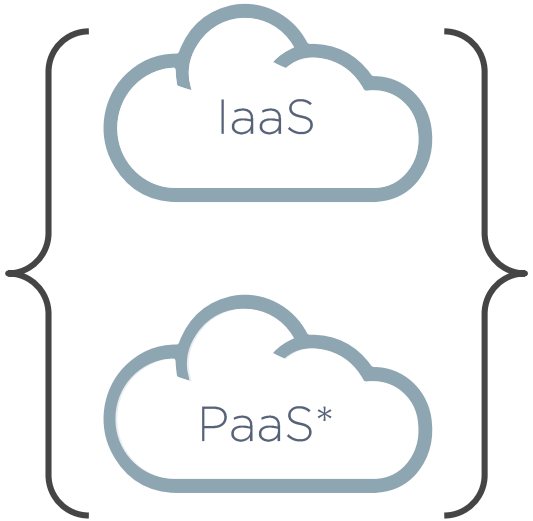
Capital One
After: Introducing Security at the Source

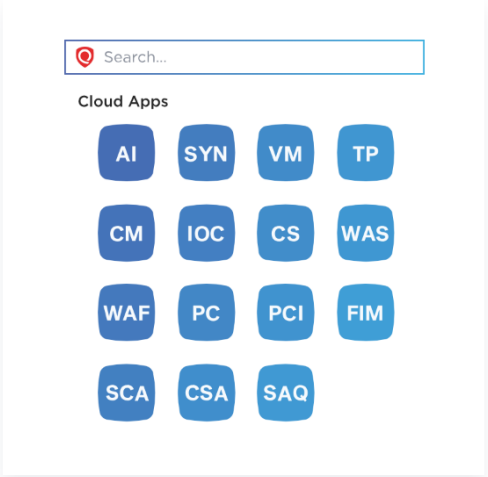
Qualys Security into Gold Images and AMI



Bakery process happens within 24 Hrs

Cloud Workload Security with Qualys





aws Azure Google Cloud Platform Alibaba Cloud aliyun.com ORACLE CLOUD SOFTLAYER an IBM Company

* PaaS – Cloud Database Scanning – Roadmap 2H '19

Cloud Infrastructure Security

Australian Insurance Company

Visibility of deployments stop misuse of keys

AWS sent a notice of compromised keys attempting to create multiple accounts in EU

Use Case

Identify the resources in EU region, find the Amazon S3 buckets which are open to public and have the keys stored

Requirement

- Identify where the deployments are located
- Identify Amazon S3 buckets that are public and fix it
- Ensure best practices are followed by IAM users of the account

Company Profile
Largest provider of Auto and Agriculture insurance

INDUSTRY: Insurance

REGION: Australia

CLOUD:
Primary Cloud - AWS
Secondary Cloud- Azure

DEPLOYMENT REGION:
Australia

SERVICES USED:
EC2, S3, RDS, EMR, Cloud Front

Qualys Cloud Inventory and Security Assessments

Unparalleled Visibility and Continuous Security Monitoring across public cloud infrastructure

aws

Azure

Google Cloud Platform

CI

Cloud Inventory

CSA

Cloud Security Assessment

Use Case #1

Visibility into your public clouds

View into

- Resource Distribution by Type
- Resources by Region

Personalize and add custom widgets

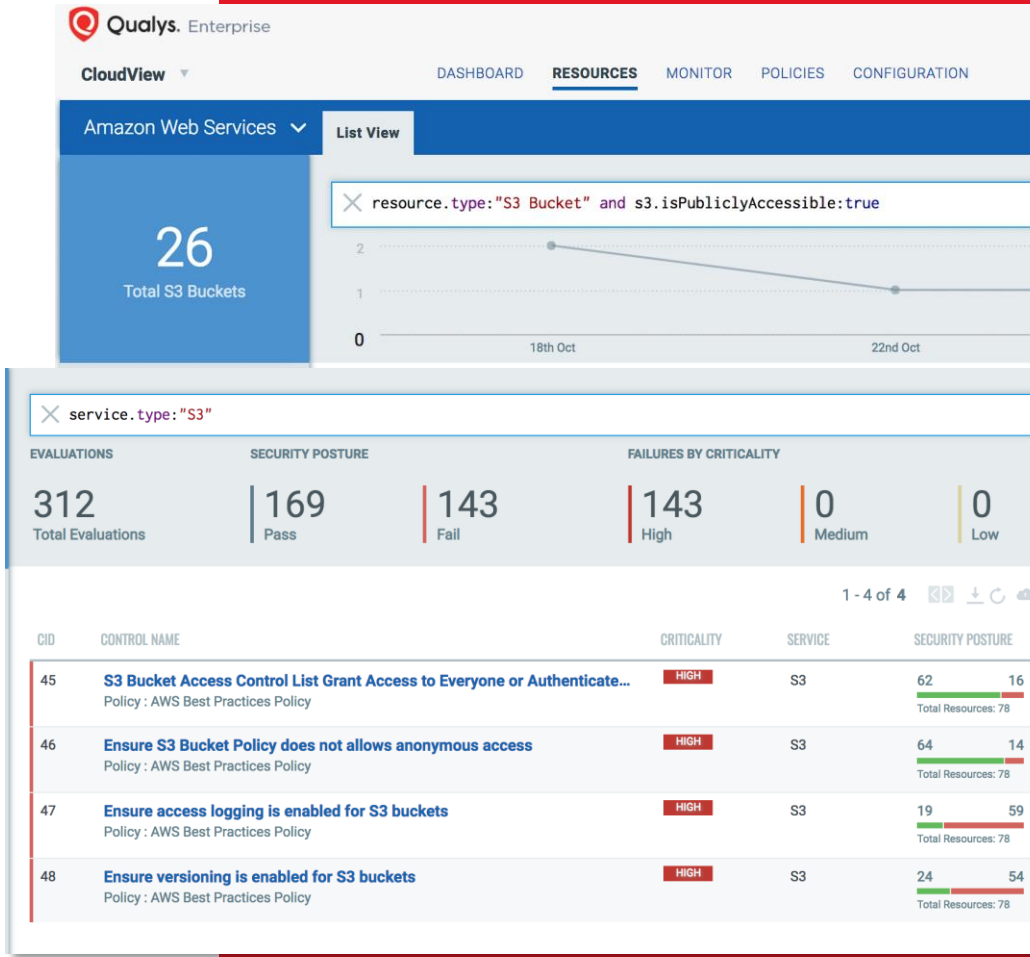
Use Case #2

Identify Leaky S3 buckets

Misconfigured S3 Buckets are vulnerable for data leaks

Check the S3 Bucket Access Permissions Regularly

- Review Access Control List
- Check Bucket Policy

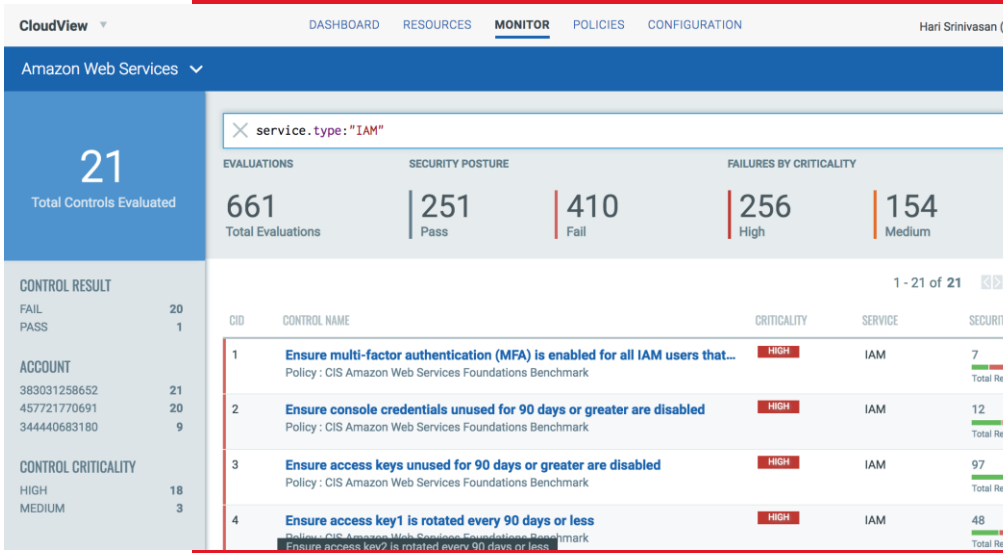


Use Case #3

Detect Compromised IAM Users

Check for:

- Configure Strong Password Policy for Account
- Enforce MFA for Console Users
- Rotate IAM Access Keys Every 90 Days
- Removed Unnecessary Credentials
- Audit Process
  - Create separate user for console & API access (Segregation of duty)
  - Track password age
  - Deactivate unused keys



Australian Insurance Company

Visibility of deployments stop misuse of keys

AWS sent a notice of compromised keys attempting to create multiple accounts in EU

Requirement

- Identify where the deployments are located
- Identify S3 buckets that are public and fix it
- Ensure best practices are followed by IAM users of the account

Solution

With Qualys Cloud Inventory and Assessment

✓ Gain visibility into the global deployments

✓ Identify S3 buckets that are public and required fixing

✓ Identify the IAM users and their security posture

Company Profile

Largest provider of Auto and Agriculture insurance

INDUSTRY: Insurance

REGION: Australia

CLOUD:
Primary Cloud - AWS
Secondary Cloud- Azure

DEPLOYMENT REGION:
Australia

SERVICES USED:
EC2, S3, RDS, EMR, Cloud Front

CloudView

A FREE inventory and monitoring service for your public clouds

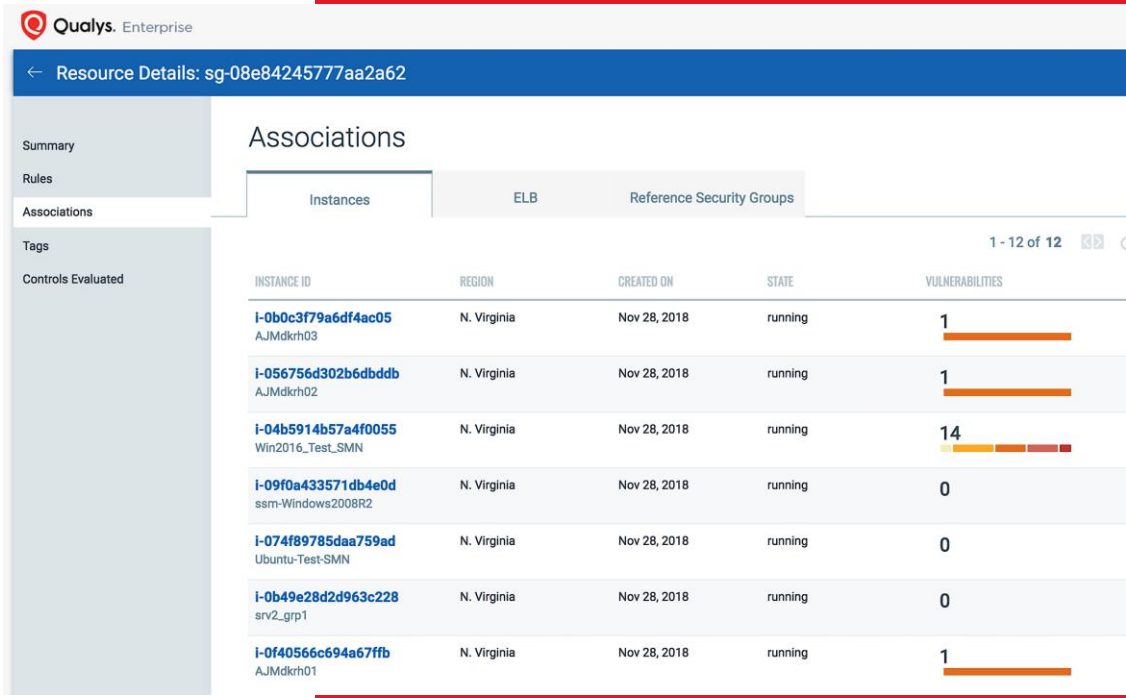
* FREE version is for Cloud Inventory, defaults to 3 accounts per cloud, can be extended further

Qualys.

Correlate with Vulnerability Data

Identify vulnerable instances associated with the security groups

Reduce effort to pull info to SIEM for correlation



Coming Jan'19

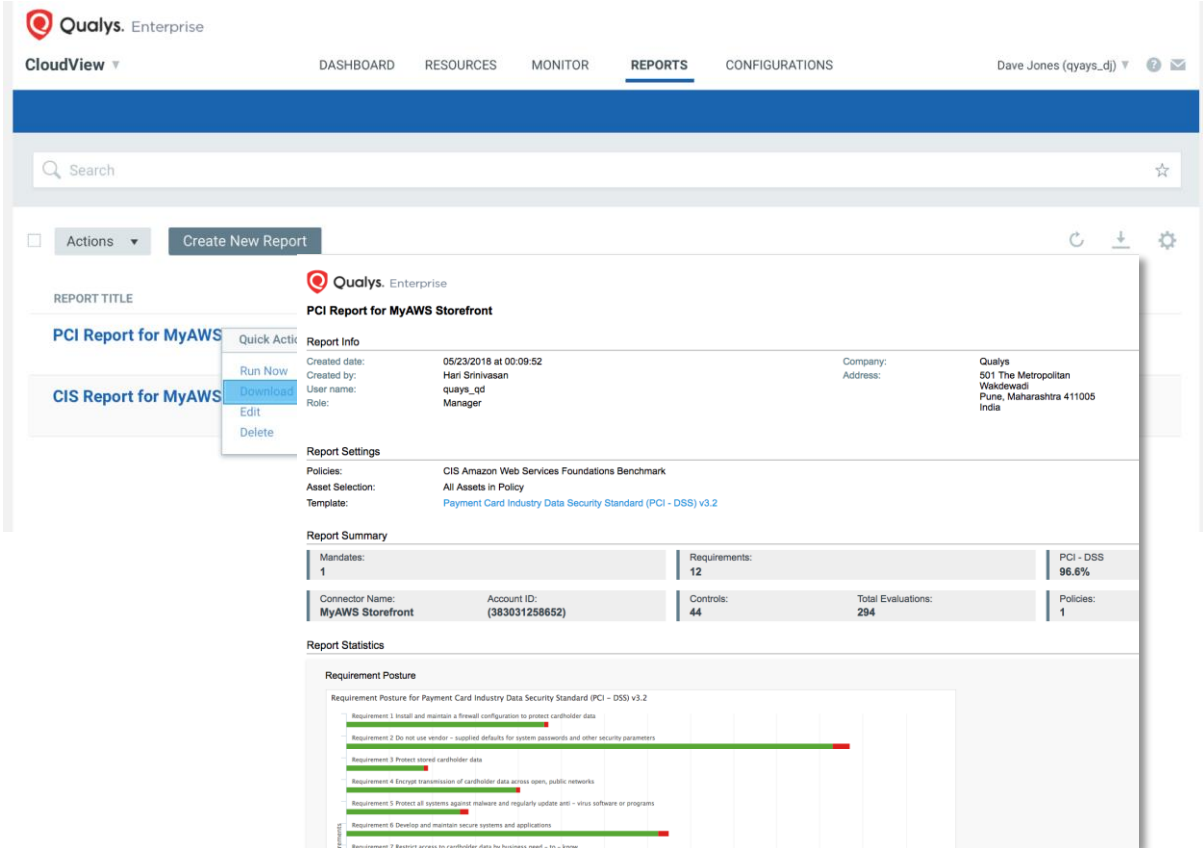
Cloud Infrastructure Reports

Generate reports for CIS Benchmarks, mandates like PCI, HIPAA, ISO27001, NIST 800-53,..

Configure for specific accounts, and regions

Schedule reports for daily, weekly or monthly

Coming May. 2019

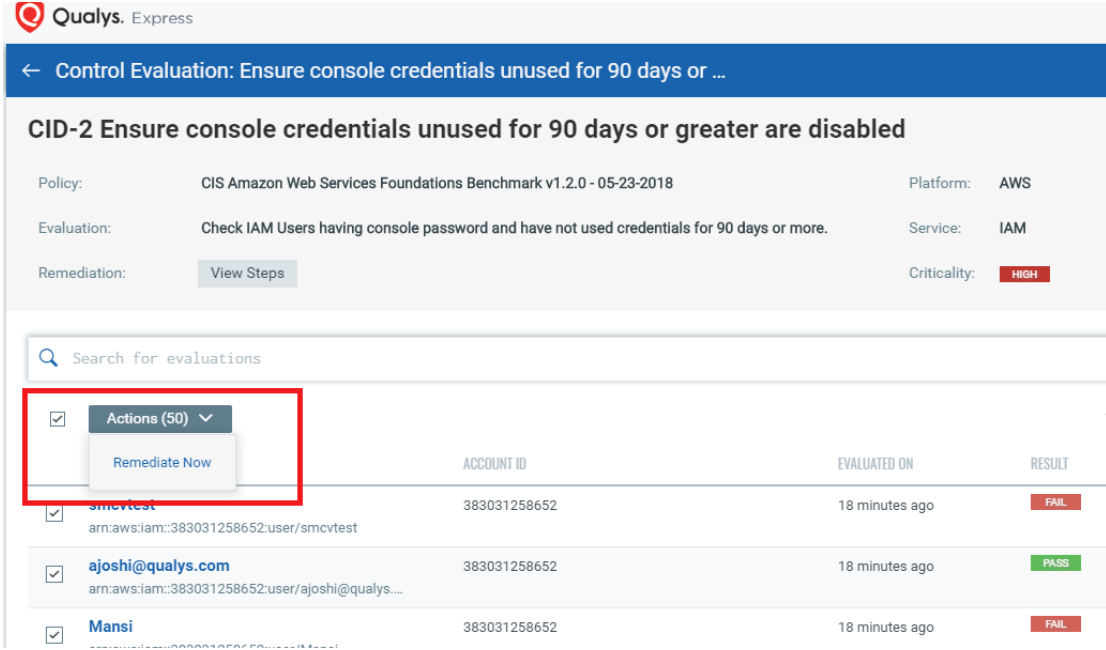


Cloud Security Management

Automated remedial actions to protect against risks

End to End flow: Setup On-demand or automated remediation to fix control failures

Scope it by account, controls, tags,..



Coming Q3 2019

Qualys.

Cloud SaaS Security

SaaS Security (SSC)

Adya.io now part of Qualys

Manage and Secure your SaaS Applications

Critical SaaS apps

Exposure of Data

For Compliance

On unused Licenses

Qualys.

SaaS Security and Compliance

Features

ADMINISTRATION

- Add /remove users from groups
- Add/ remove users from channels
- Role based access control
- onboarding / offboarding workflows

SECURITY & COMPLIANCE

- External / internal data exposure
- One click exposure fix
- List / fix dangerous apps
- Alert on exposure / dangerous apps

LICENCE MANAGEMENT

- Central visibility into SaaS licenses
- See underutilized licenses
- Understand total cost / savings
- Future spend analysis

REPORT & AUDIT

- Activity logs by user / group
- Access reports for files / folder
- On-demand / scheduled reports
- Pre-built / scheduled reports

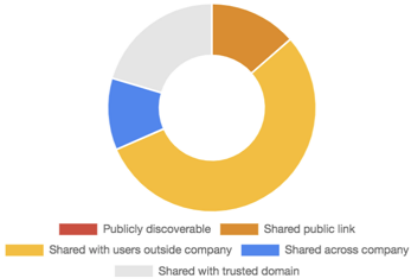
Qualys | Dashboard | Users | Documents | Apps | Policies | Reports | Testing (testuser@adya.io)

10 USERS

22 GROUPS

20022 FILES

1350 FOLDERS



618 Shared documents

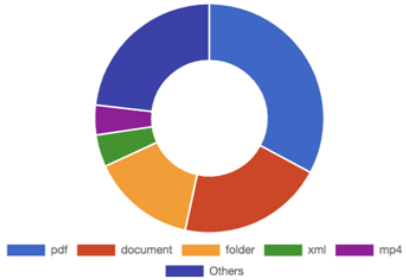
External users with most access

neetika@accelero-corp.com	142
deepakbalakrishna@gmail.com	34
dbalakrishna@qualys.com	22
nasar@qualys.com	21
sthakar@qualys.com	21

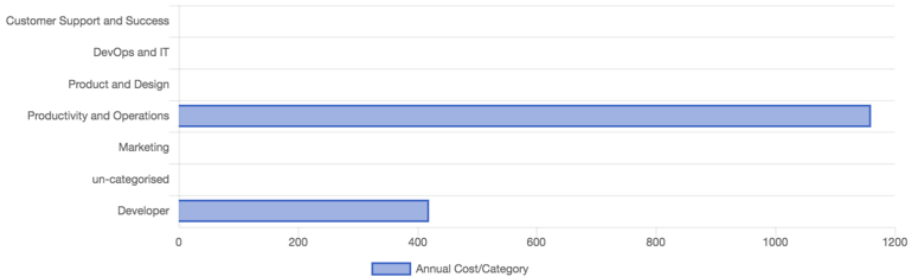
...and 19 more

Users with most exposed documents

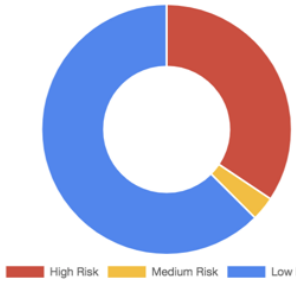
deepak@adya.io	335
scm@adya.io	3
rashmi.singh@adya.io	1



618 Files Exposed



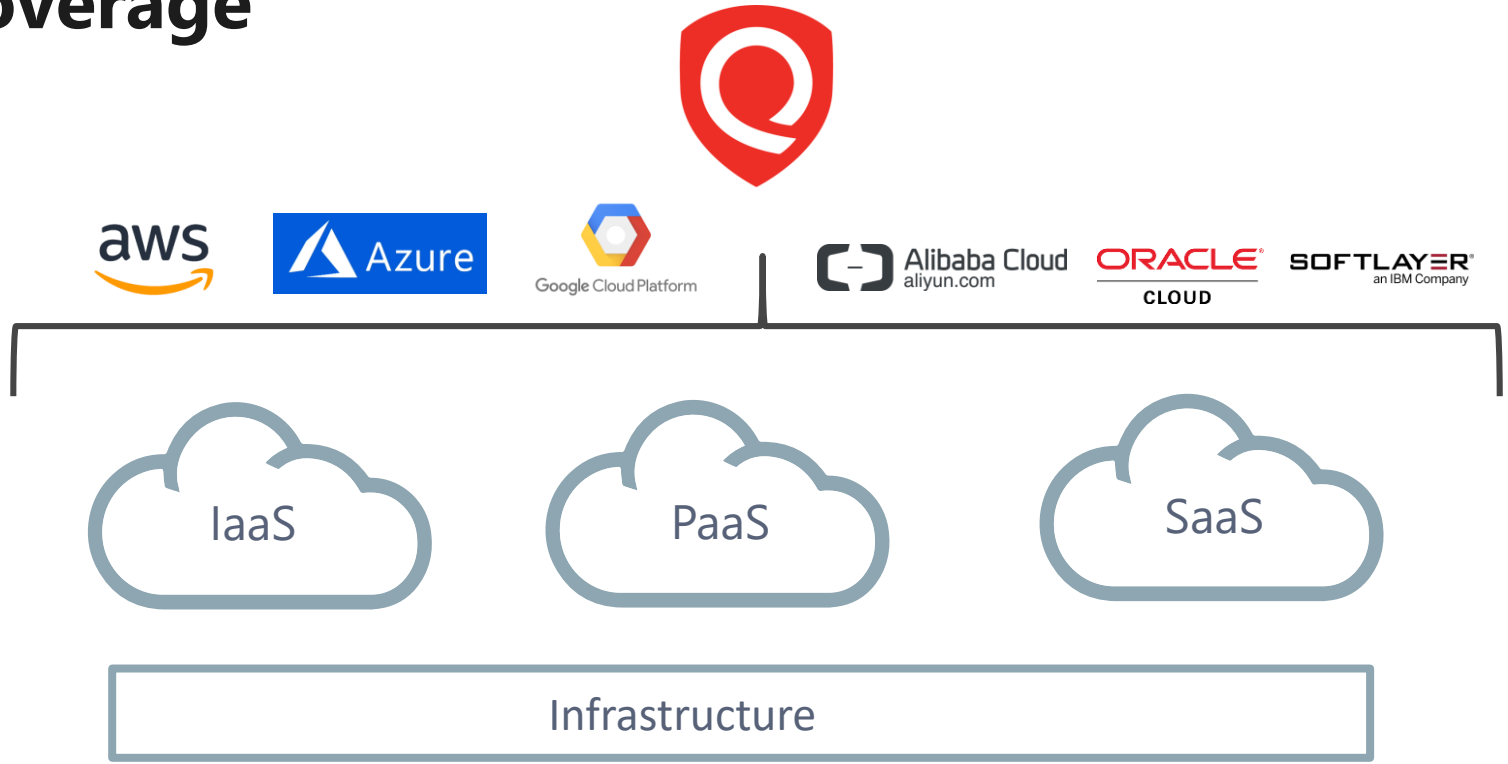
1580.4 $ in Total Annual Cost



32 installed Apps

Qualys.

Qualys Cloud Security – Comprehensive Coverage



* PaaS – Cloud Database Scanning – Roadmap ‘19
* SaaS – Qualys acquired Adya.io Feb’19. Security for GSuite, Slack, O365,..

Q&A